Discussion on the ideal of program-correctness by Tony Hoare

Article

Published Version

The Ideal of Program Correctness

Third Computer Journal Lecture

TONY HOARE

Discussion on The Ideal of Program Correctness by Tony Hoare

9. GUY HAWORTH

School of Systems Engineering, University of Reading, UK.
Email: g.haworth@reading.ac.uk

(i) What examples are there of achievements in showing Program Correctness? Are any of these in a non-discrete domain?
(I asked the speaker this after the meeting. He mentioned work done on the Ariane software system after the loss of a satellite. Since this software used floating-point numbers, we classify this as not being in a discrete domain.)

(ii) What are the leading methods and tools for Program Verification today?

From: The Computer Journal, 50.3 (2007)
pp. 254–260, 261–268
and 269-273

(iii) It seems that if program P is to be formally verified from specification S, then S (as well as P) are expressed in a formal language.
Working back, it seems that any formal verification must start with a formal statement in a formal language.
Therefore, all formal verification is done in a 'formal world' of formal statements and formal verification methods.
Since the room here is in two parts, let us designate that side of the room with Leading Computer Scientists in as 'the formal world'.
However, requirements for systems are originally expressed using informal, natural languages, such as English.
These languages are flexible and therefore have their ambiguities and dangers.
Further, at some point, there is a 'last' expression of requirements in natural language and a 'first' expression in a formal language.
It would seem impossible to do better than to have the translation of the one to the other signed off by a domain expert as no formal verification is possible.
Is this a fair assessment of the situation?

Discussion on The Ideal of Program Correctness: Responses from Tony Hoare

TO GUY HAWORTH

(i) The answers to these questions may be found in a 'roadmap' document being assembled at `http://qpq.csl.sri.com/vsr/private/verified-software-roadmap-2006/Overview`

(ii) See the website referenced above, or www.qpq.org/modules

(iii) Your assessment of the situation is very fair.